BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problems Mailbox.

```
File   2:INSPEC 1969-2003/Dec W1
         (c) 2003 Institution of Electrical Engineers
File   6:NTIS 1964-2003/Dec W3
         (c) 2003 NTIS, Intl Cpyrght All Rights Res
File   8:Ei Compendex(R) 1970-2003/Dec W2
         (c) 2003 Elsevier Eng.  Info. Inc.
File  34:SciSearch(R) Cited Ref Sci 1990-2003/Dec W3
         (c) 2003 Inst for Sci Info
File  35:Dissertation Abs Online 1861-2003/Nov
         (c) 2003 ProQuest Info&Learning
File  65:Inside Conferences 1993-2003/Dec W3
         (c) 2003 BLDSC all rts. reserv.
File  94:JICST-EPlus 1985-2003/Dec W3
         (c)2003 Japan Science and Tech Corp(JST)
File  95:TEME-Technology & Management 1989-2003/Dec W1
         (c) 2003 FIZ TECHNIK
File  99:Wilson Appl. Sci & Tech Abs 1983-2003/Nov
         (c) 2003 The HW Wilson Co.
File 111:TGG Natl.Newspaper Index(SM) 1979-2003/Dec 19
         (c) 2003 The Gale Group
File 144:Pascal 1973-2003/Dec W2
         (c) 2003 INIST/CNRS
File 202:Info. Sci. & Tech. Abs. 1966-2003/Nov 17
         (c) 2003 EBSCO Publishing
File 233:Internet & Personal Comp. Abs. 1981-2003/Jul
         (c) 2003, EBSCO Pub.
File 266:FEDRIP 2003/Oct
         Comp & dist by NTIS, Intl Copyright All Rights Res
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
File 483:Newspaper Abs Daily 1986-2003/Dec 22
         (c) 2003 ProQuest Info&Learning
File 583:Gale Group Globalbase(TM) 1986-2002/Dec 13
         (c) 2002 The Gale Group
File 256:SoftBase:Reviews,Companies&Prods. 82-2003/Nov
         (c)2003 Info.Sources Inc
? ds

Set     Items   Description
S1    2581212   MANUFACTUR??? ? OR PRODUCER? ? OR PRODUCING OR SUPPLIER? OR
               SUPPLYING
S2    2468400   KEY? ? OR ALGORITHM? ? OR CIPHER? ? OR CYPHER? ?
S3      12083   PRIVATEKEY? OR (PRIVATE OR SECRET OR SYMMETRIC OR CONVENTI-
               ONAL)(1W)S2
S4       9822   (SERIAL OR UNIQUE)(2N)(IDENTIFIER? ? OR NUMBER? ? OR NUMER-
               IC?? ? OR NUMERAL? ? OR CODE OR CODES OR CODING?)
S5      10414   (UNIT OR MODULE OR COMPONENT OR DEVICE OR APPARAT? OR APP??
               ? OR EQUIPMENT OR APPLIANCE)(1W)(IDENTIFER? ? OR NUMBER? ? OR
               NUMERIC?? ? OR NUMERAL? OR CODE? ? OR CODING?)
S6         26   (SET()TOP OR SETTOP OR MEDIAPLAYER? OR (MULTIMEDIA OR MEDIA
               OR REAL OR FREE)()PLAYER? OR QUICKTIME OR FREEPLAYER?)(1W)(I-
               DENTIFER? ? OR NUMBER? ? OR NUMERIC?? ? OR NUMERAL? OR CODE? ?
               OR CODING?)
S7        253   (QUICK()TIME OR REALPLAYER? OR REALAUDIO OR REAL()AUDIO)(1-
               W)(IDENTIFER? ? OR NUMBER? ? OR NUMERIC?? ? OR NUMERAL? OR CO-
               DE? ? OR CODING?) OR UID OR UIDS
S8     285758   LICENS??? ? OR LICENC??? ?
S9        896   S8(7N)S2
S10        90   S9 AND S1
S11         2   S10 AND S3
S12         2   S10 AND S4:S7
```

S13 0 S11 AND S12
S14 4 S11:S12
S15 2 S14/2000:2003
S16 2 S14 NOT S15
S17 2 RD (unique items)
? t17/7/2

17/7/2 (Item 1 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00531514 99PK04-207
Microsoft beta `jams' in RealNetworks' arena
Rapoza, Jim
PC Week , April 19, 1999 , v16 n16 p14, 1 Page(s)
ISSN: 0740-1604
Company Name: Microsoft
URL: http://www.microsoft.com
Product Name: Microsoft Windows Media Technologies 4.0

Presents a favorable review of Windows Media Technologies 4.0 beta ($NA), an Internet streaming media platform suite from Microsoft Corp. of Redmond, WA (800). Explains that it includes a new version of the Windows Media Player. Cites features such as high-quality audio and video streaming, rights management tool, an On-Demand **Producer** that allows the editing of audio and video files before encoding, public- and **private - key** encryption to manage user **licenses** to media, system ID number, and improved authoring tools. However, it has inadequate format conversion support, and users are unable to encode once for multiple connection types. Concludes that it has the potential to raise the bar in music distribution. Includes one screen display and one product summary. (MEM)
?

```
File 696:DIALOG Telecom. Newsletters 1995-2003/Dec 22
         (c) 2003 The Dialog Corp.
File  15:ABI/Inform(R) 1971-2003/Dec 23
         (c) 2003 ProQuest Info&Learning
File 141:Readers Guide 1983-2003/Nov
         (c) 2003 The HW Wilson Co
File 484:Periodical Abs Plustext 1986-2003/Dec W1
         (c) 2003 ProQuest
File 813:PR Newswire 1987-1999/Apr 30
         (c) 1999 PR Newswire Association Inc
File 613:PR Newswire 1999-2003/Dec 23
         (c) 2003 PR Newswire Association Inc
File 635:Business Dateline(R) 1985-2003/Dec 23
         (c) 2003 ProQuest Info&Learning
File 810:Business Wire 1986-1999/Feb 28
         (c) 1999 Business Wire
File 610:Business Wire 1999-2003/Dec 23
         (c) 2003 Business Wire.
File 369:New Scientist 1994-2003/Dec W2
         (c) 2003 Reed Business Information Ltd.
File 370:Science 1996-1999/Jul W3
         (c) 1999 AAAS
File  20:Dialog Global Reporter 1997-2003/Dec 23
         (c) 2003 The Dialog Corp.
File 624:McGraw-Hill Publications 1985-2003/Dec 22
         (c) 2003 McGraw-Hill Co. Inc
File 634:San Jose Mercury  Jun 1985-2003/Dec 21
         (c) 2003 San Jose Mercury News
File 647:CMP  Computer Fulltext 1988-2003/Dec W3
         (c) 2003 CMP Media, LLC
File 674:Computer News Fulltext 1989-2003/Dec W1
         (c) 2003 IDG Communications
? ds

Set     Items   Description
S1    3653079   MANUFACTUR??? ?
S2    3394767   KEY? ? OR ALGORITHM? ? OR CIPHER? ? OR CYPHER? ?
S3       6900   PRIVATEKEY? OR (PRIVATE OR SECRET OR SYMMETRIC OR CONVENTI-
             ONAL)(1W)S2
S4      29804   (SERIAL OR UNIQUE)(2N)(IDENTIFIER? ? OR NUMBER? ? OR NUMER-
             IC?? ? OR NUMERAL? ?)
S5       4789   (UNIT OR MODULE OR COMPONENT OR DEVICE OR APPARAT? OR APP??
              ? OR EQUIPMENT OR APPLIANCE)(1W)(IDENTIFER? ? OR NUMBER? ? OR
              NUMERIC?? ? OR NUMERAL?)
S6         12   (SET()TOP OR SETTOP OR MEDIAPLAYER? OR (MULTIMEDIA OR MEDIA
             OR REAL OR FREE)()PLAYER? OR QUICKTIME OR FREEPLAYER?)(1W)(I-
             DENTIFER? ? OR NUMBER? ? OR NUMERIC?? ? OR NUMERAL?)
S7          6   (QUICK()TIME OR REALPLAYER? OR REALAUDIO OR REAL()AUDIO)(1-
             W)(IDENTIFER? ? OR NUMBER? ? OR NUMERIC?? ? OR NUMERAL?)
S8    2100265   LICENS??? ? OR LICENC??? ?
S9        466   UID OR UIDS
S10      4137   (SERIAL OR UNIQUE)(2N)(CODE OR CODES)
S11       193   (SERIAL OR UNIQUE)(2N)CODING? ?
S12      2154   (UNIT OR MODULE OR COMPONENT OR DEVICE OR APPARAT? OR APP??
              ? OR EQUIPMENT OR APPLIANCE)(1W)(CODE OR CODES OR CODING?)
S13       132   (SET()TOP OR SETTOP OR MEDIAPLAYER? OR (MULTIMEDIA OR MEDIA
             OR REAL OR FREE)()PLAYER? OR QUICKTIME OR FREEPLAYER?)(1W)(C-
             ODE? ? OR CODING?)
S14        20   (QUICK()TIME OR REALPLAYER? OR REALAUDIO OR REAL()AUDIO)(1-
             W)(CODE? ? OR CODING?)
S15   3179817   PRODUCER? ? OR PRODUCING OR SUPPLIER? OR SUPPLYING
```

S16 14760 S8(7N)S2
S17 1939 (S1 OR S15)(S)S16
S18 3 S17(S)S3
S19 6 S17(S)(S4:S7 OR S9:S14)
S20 1 S18 AND S19
S21 8 S18:S20
S22 5 S21/2000:2003
S23 3 S21 NOT S22
S24 3 RD (unique items)
? t24/3,k/1,3

24/3,K/1 (Item 1 from file: 696)
DIALOG(R)File 696:DIALOG Telecom. Newsletters

00674138
EXPLOITING BROADBAND CAPABILITY
TELECOMS STANDARDS & APPROVALS REVIEW
May 20, 1999 DOCUMENT TYPE: NEWSLETTER
PUBLISHER: PHILLIPS BUSINESS INFORMATION
LANGUAGE: ENGLISH WORD COUNT: 1637 RECORD TYPE: FULLTEXT

TEXT:
...and recent announcements show that
Microsoft is anxious to challenge Oracle, currently the main software **supplier** for black boxes. It is likely that whoever gains a stronghold in the UK will...

...standard.

Electronic signatures
Electronic commerce is well established between companies having close relationships, eg a **manufacturer** and its main **suppliers**, operating over a private communication link. The key issue now is whether commercial transactions are...

...well as legalising digital signatures.
Note: An "electronic signature" is a document which provides a **unique identifier** for each party in an on-line transaction. It confirms the agreement of each party...

...issues users with a
"digital certificate" confirming the authenticity of the signatures and providing the **private key** to the basic public key/ **private key** encryption system.

Encouragement for electronic trade
At the beginning of March the UK government issued...government proposals to insist upon the use of a
key escrow system, with third party **key** recovery, as part of the **licensing** scheme.
The industry has argued that making this a mandatory requirement under the licensing scheme...

24/3,K/3 (Item 1 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext

01189937 CMP ACCESSION NUMBER: WIN19990501S0008
Chipping Away at Our Privacy - Two recent events-one overt, one not-illustrate just how easy it is to lose your PC privacy. (The Explorer)
Fred Langa
WINDOWS MAGAZINE, 1999, n 1005, PG21
PUBLICATION DATE: 990501
JOURNAL CODE: WIN LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: Analysis
WORD COUNT: 1018

TEXT:

You've probably heard about Intel's plan to embed an individual " processor **serial number** " (PSN) in each machine running on a Pentium III (PIII) chip. The 96-bit ID...

...this kind of identification: Resource- tracking within an enterprise is one example. Indeed, some workstation **manufacturers** already feature similar functions. And while some apps use **serial numbers** for **licensing** , other software uses hardware-based " dongles" (" **keys** " that attach to a parallel or serial port) for the same purpose.
?

File 347:JAPIO Oct 1976-2003/Aug(Updated 031202)
(c) 2003 JPO & JAPIO
File 350:Derwent WPIX 1963-2003/UD,UM &UP=200381
(c) 2003 Thomson Derwent
File 348:EUROPEAN PATENTS 1978-2003/Dec W02
(c) 2003 European Patent Office
File 349:PCT FULLTEXT 1979-2002/UB=20031218,UT=20031211
(c) 2003 WIPO/Univentio
? ds

Set	Items	Description
S1	14	AU='GOLDSCHLAG D':AU='GOLDSCHLAG DAVID M'
S2	3	AU='KRAVITZ D'
S3	18	AU='KRAVITZ D W':AU='KRAVITZ DAVID'
S4	17	AU='KRAVITZ DAVID W':AU='KRAVITZ DAVID WILLIAM'
S5	10	S1 AND S2:S4
S6	24705	LICENS? OR LICENC?
S7	5	S1:S4 AND S6
S8	1	S5 AND S6
S9	5	S7:S8
S10	1975171	MANUFACTUR?
S11	6	S1:S4 AND S10
S12	8	S9 OR S11

? t12/5/all

12/5/1 (Item 1 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00906077 **Image available**
SYSTEM AND METHOD FOR MANAGING TRUST BETWEEN CLIENTS AND SERVERS
SYSTEME POUR GERER LA CONFIANCE ENTRE DES CLIENTS ET DES SERVEURS
Patent Applicant/Assignee:
WAVE SYSTEMS CORPORATION, Suite B200, 480 Pleasant Street, Lee, MA 01238, US, US (Residence), US (Nationality)
Inventor(s):
KRAVITZ David W , 3910 Ridgelea Drive, Fairfax, VA 22031, US
Legal Representative:
BUTTER Gary M (et al) (agent), Baker Botts, LLP, 30 Rockefeller Plaza, New York, NY 10112-0228, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200239222 A2-A3 20020516 (WO 0239222)
Application: WO 2001US46238 20011019 (PCT/WO US0146238)
Priority Application: US 2000242083 20001020; US 2000246843 20001108
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PH PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: G06F-017/60
International Patent Class: H04K-001/00; H04L-009/00
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 11769

English Abstract
A method and architecture that enables consumers to computer data from multiple providers without jeoparadizing consumer privacy interests or intellectual property rights of providers is disclosed. The architecture includes a trust server (150) that mediates the conferral and revocation of trust relationships between the two parties. The method also employs programmable security coprocessors (170) at vulnerable sites requiring protection, namely at the trust server (150) and at each consumer (110). The architecture further reflects the specific requirements of coprocessors within consumer-side installations and their server-side counterparts. A single coprocessor (170) within a client platform (110) serves multiple providers by allocating to each of them a virtualized trusted computing environment for software execution and data manipulation. Since the tamper-resistance offered by client-side coprocessors (170) is subject to more stringent economic pressures than that offered by server-side hardware security modules (160), the architecture includes containment capabilities that prevent compromised coprocessors from causing damage disproportionate to their numbers.

French Abstract
L'invention concerne un procede et une architecture permettant a des consommateurs d'acceder a des donnees informatiques provenant de multiples fournisseurs sans que les interets prives des consommateurs ou les droits de propriete intellectuelle des fournisseurs n'en souffrent. Cette architecture comprend un serveur de confiance qui sert d'intermediaire pour l'etablissement et la suppression de relations de confiance entre les deux parties. Ledit procede fait egalement appel a des coprocesseurs de securite programmables se trouvant en des sites vulnerables exigeant une protection, notamment au niveau de chaque serveur de confiance et de chaque consommateur. L'architecture prend en compte les exigences specifiques de coprocesseurs dans des installations cote client et dans les installations correspondantes cote serveur. Un seul coprocesseur se trouvant dans une plate-forme client sert plusieurs fournisseurs en assignant a chacun d'eux un environnement de calcul de confiance virtualise pour l'execution de logiciels et la manipulation de donnees. Etant donne que la resistance aux fraudes offerte par les coprocesseurs cote client est soumise a des pressions economiques plus fortes que celles auxquelles est soumise la resistance aux fraudes offerte par les modules de securite materiels cote serveur (HSM), l'architecture presente des capacites de confinement qui empechent des coprocesseurs compromis de provoquer des dommages disproportionnes par rapport a leur nombre.

Legal Status (Type, Date, Text)
Publication 20020516 A2 Without international search report and to be republished upon receipt of that report.
Search Rpt 20030306 Late publication of international search report
Republication 20030306 A3 With international search report.

12/5/2 (Item 2 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00578019 **Image available**
CONTENT PACKET DISTRIBUTION SYSTEM
SYSTEME DE DISTRIBUTION DE PAQUETS DE CONTENU
Patent Applicant/Assignee:
DIGITAL VIDEO EXPRESS L P,
SCHUMANN Robert,
GOLDSHLAG David,

KRAVITZ David,
IU Siu-Leong,
MERCIER Guillaume,
WHITTEMORE Richard,
BERGERON Michael,
EHRHARDT Jack,
VITKUS Richard,
Inventor(s):
SCHUMANN Robert,
GOLDSHLAG David,
KRAVITZ David ,
IU Siu-Leong,
MERCIER Guillaume,
WHITTEMORE Richard,
BERGERON Michael,
EHRHARDT Jack,
VITKUS Richard
Patent and Priority Information (Country, Number, Date):
Patent: WO 200041392 A1 20000713 (WO 0041392)
Application: WO 2000US79 20000105 (PCT/WO US0000079)
Priority Application: US 99114833 19990106
Designated States: AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZA ZW GH GM KE LS MW SD SL SZ TZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
Main International Patent Class: H04N-007/24
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 12907

English Abstract
A transport packet generation apparatus and method used in a system which delivers content such as movies and music is disclosed. This invention provides a mechanism for providing and retrieving content on a medium such as a DVD optical disc. One aspect of the present invention provides content by processing and packing data packets onto the medium. A further aspect of the present invention retrieves content by reading data off the medium and processing the data to functionally reconstruct the original data packets for use in the system for delivering content.

French Abstract
Selon cette invention, un appareil de generation de paquets de transport et un procede correspondant sont utilises dans un systeme qui fournit un contenu tel que des films ou de la musique. L'invention concerne un mecanisme pour fournir et recuperer du contenu sur un support tel qu'un disque optique DVD. Dans l'un des aspects, on fournit le contenu en traitant et en empaquetant les paquets de donnees sur le support. Dans un autre aspect de l'invention, le contenu est recupere par la lecture des donnees a partir du support et par leur traitement permettant la reconstruction fonctionnelle des paquets de donnees d'origine, utilises dans le systeme pour fournir du contenu.

12/5/3 (Item 3 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00577683 **Image available**

DIGITAL CONTENT DISTRIBUTION SYSTEM AND METHOD

SYSTEME ET PROCEDE DE DISTRIBUTION DE CONTENU NUMERIQUE

Patent Applicant/Assignee:
DIGITAL VIDEO EXPRESS L P,
SCHUMANN Robert,
GOLDSCHLAG David,
KRAVITZ David,
IU Siu-Leong,
MERCIER Guillaume,
WHITTEMORE Richard,
BERGERON Michael,
EHRHARDT Jack,
VITKUS Richard,

Inventor(s):
SCHUMANN Robert,
GOLDSCHLAG David ,
KRAVITZ David ,
IU Siu-Leong,
MERCIER Guillaume,
WHITTEMORE Richard,
BERGERON Michael,
EHRHARDT Jack,
VITKUS Richard

Patent and Priority Information (Country, Number, Date):
Patent: WO 200041056 A2 20000713 (WO 0041056)
Application: WO 2000US77 20000105 (PCT/WO US0000077)
Priority Application: US 99114833 19990106

Designated States: AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZA ZW GH GM KE LS MW SD SL SZ TZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG

Main International Patent Class: H04N-007/167
International Patent Class: H04N-005/00
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 12132

English Abstract

A content distribution system and method which prevents unauthorized access to secured content such as movies and music. The apparatus includes a source, a receiver, an authorized security device such as a conditional access module (CAM) for decrypting authorized content, an output device for outputting content and a backend for managing accounts and system operations. One aspect of this invention provides a mechanism for providing secured content on a medium such as a DVD optical disc. These devices may verify that there is authorization to play the secured content, add watermarks to the secured content, convert the secured content to a displayable form and provide a means for preventing output of the secured content.

French Abstract

L'invention concerne un systeme et un procede de distribution de contenu numerique qui empechent tout acces non autorise a un contenu securise tel que de la musique ou des films. L'appareil comprend une source, un recepteur, un dispositif de securite autorise tel qu'un module d'acces conditionnel, ou MAC, destine a dechiffrer le contenu autorise, un

dispositif de sortie destine a emettre le contenu et un systeme principal charger de gerer les comptes et d'effectuer les operations systeme. Dans l'un des aspects, l'invention concerne un mecanisme pour livrer un contenu securise sur un support tel qu'un disque optique DVD. Ces dispositifs peuvent verifier la presence d'une autorisation de lire le contenu securise, ajouter des filigranes au contenu securise, convertir le contenu securise en une forme affichable et fournir des moyens empechant d'emettre le contenu securise.

12/5/4 (Item 4 from file: 349)

00511768 **Image available**

INFORMATION ACCESS CONTROL SYSTEM AND METHOD
SYSTEME ET PROCEDE DE CONTROLE D'ACCES A DES INFORMATIONS

Patent Applicant/Assignee:
DIGITAL VIDEO EXPRESS L P,
GOLDSCHLAG David M,
KRAVITZ David W,
Inventor(s):
GOLDSCHLAG David M ,
KRAVITZ David W

Patent and Priority Information (Country, Number, Date):
Patent: WO 9943120 A1 19990826
Application: WO 99US3275 19990219 (PCT/WO US9903275)
Priority Application: US 9875433 19980220; US 9881766 19980415; US 9881739 19980415; US 9897845 19980825; US 98110021 19981125; US 99116002 19990115
Designated States: AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZW GH GM KE LS MW SD SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
Main International Patent Class: H04K-001/00
International Patent Class: H04K-001/02; H04N-007/167
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 21949

English Abstract
An information access control system and method which prevents unauthorized access from accessing the information. The apparatus includes a set top box (100) which receives the information from a broadcast stream or recorded medium, or other source and a conditional access module. The set top box (100) is paired with the conditional access module (400) such that they have a shared secret key which is used to send communications to each other. A pirate attempting unauthorized access does not have the shared secret key and thus can not receive the communications. The apparatus and method further require that the set top box (100) and the conditional access module (400) follow one of a plurality of protocols in communicating with each other. A pirate attempting unauthorized access will not able to follow the protocols.

French Abstract
L'invention concerne un systeme et un procede de controle d'acces a des informations, destine a empecher tout acces non autorise a ces

informations. L'appareil de cette invention comprend un boitier decodeur (STP) (100) qui recoit lesdites informations depuis un flux diffuse, un support d'enregistrement, ou toute autre source, et un module d'acces conditionnel (CAM). Le boitier decodeur (100) est couple a ce module (400) d'acces conditionnel, de sorte que ce boitier et ce module partagent une cle secrete qu'ils utilisent pour echanger des informations. Un pirate tentant un acces non autorise sans posseder cette cle secrete ne sera donc pas en mesure de recevoir les communications echangees. Selon l'appareil et le procede de cette invention, ledit boitier decodeur (100) et ledit module (400) d'acces conditionnel doivent suivre un protocole choisi parmi plusieurs protocoles afin de pouvoir communiquer, alors qu'un pirate faisant une tentative d'acces non autorise ne pourra se conformer a ces protocoles.

12/5/5 (Item 5 from file: 349)

00511613 **Image available**

COMPUTER-BASED METHOD AND SYSTEM FOR AIDING TRANSACTIONS
PROCEDE ET SYSTEME INFORMATIQUES D'AIDE AUX TRANSACTIONS

Patent Applicant/Assignee:
CERTCO,
FRANKEL Yair,
KRAVITZ David William,
MONTGOMERY Charles Thomas,
YUNG Marcel Mordechay,
Inventor(s):
FRANKEL Yair,
KRAVITZ David William ,
MONTGOMERY Charles Thomas,
YUNG Marcel Mordechay

Patent and Priority Information (Country, Number, Date):
Patent: WO 9942965 A1 19990826
Application: WO 99US1877 19990218 (PCT/WO US9901877)
Priority Application: US 9826466 19980219
Designated States: AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZW GH GM KE LS MW SD SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
Main International Patent Class: G07F-019/00
International Patent Class: G06F-017/60
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 6522

English Abstract
A method for providing a warranty relating to a transaction between two parties, each party having a data communications device, in a system which includes an infrastructure composed of a plurality of locations each associated with a respective institution which provides services to clients, each location having a computer system, a database coupled to the computer system and storing information about each client of the institution and a data communications device coupled to the computer system for communication with the data communications device of any one party, each party being a client of at least one of the institutions, the

method containing the steps of: transmitting a request for a warranty from one party to the transaction which is a client of the respective institution to a respective location associated with the respective institution, which request includes information identifying the other party to the transaction and information about the nature of the transaction; conducting an exchange of information between the respective location and a location associated with an institution of which the other party is a client; and transmitting a response to the request from the respective location to the one party.

French Abstract
L'invention concerne un procede destine a fournir une garantie d'une transaction entre deux parties, chaque partie ayant un dispositif de communication de donnees, dans un systeme comprenant une infrastructure composee d'une pluralite d'emplacements associes chacun a une institution respective fournissant des services a des clients, chaque emplacement ayant un systeme informatique, une base de donnees couplee au systeme informatique et stockant des informations relatives a chaque client de l'institution, ainsi qu'un dispositif de communication de donnees couple au systeme informatique afin de communiquer avec le dispositif de communication de donnees de n'importe quelle partie, chaque partie etant un client d'au moins une des institutions. Le procede comprend les etapes consistant a transmettre une demande de garantie d'une partie a la transaction, laquelle est un client de l'institution respective, a l'emplacement respectif associe a l'institution respective, laquelle demande comprend des informations identifiant l'autre partie a la transaction ainsi que des informations relatives a la nature de la transaction, a effectuer un echange d'informations entre l'emplacement respectif et un emplacement associe a une institution dont l'autre partie est cliente, et a transmettre une reponse a la demande de l'emplacement respectif, a l'autre partie.

12/5/6 (Item 6 from file: 349)

00452688 **Image available**

ELECTRONIC CRYPTOGRAPHIC PACKING
TASSEMENT CRYPTOGRAPHIQUE ELECTRONIQUE

Patent Applicant/Assignee:
CERTCO LLC,
Inventor(s):
SUDIA Frank W,
ASAY Alan,
BRICKELL Ernest F,
ANKNEY Richard,
FREUND Peter C,
YUNG Marcel M,
KRAVITZ David W

Patent and Priority Information (Country, Number, Date):
Patent: WO 9843152 A1 19981001
Application: WO 98US4329 19980323 (PCT/WO US9804329)
Priority Application: US 97822732 19970324
Designated States: AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH GM GW HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZW GH GM KE LS MW SD SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN ML MR NE SN TD TG
Main International Patent Class: G06F-001/00

Publication Language: English
Fulltext Availability:
  Detailed Description
  Claims
Fulltext Word Count: 14460

English Abstract
A method of unwrapping wrapped digital data that is unusable while wrapped, includes obtaining an acceptance phrase from a user; deriving a cryptographic key from the acceptance phrase; and unwrapping the package of digital data using the derived cryptographic key. The acceptance phrase is a phrase entered by a user in response to information provided to the user. The information and the acceptance phrase can be in any appropriate language. The digital data includes, alone or in combination, any of: software, a cryptographic key, an identifying certificate, an authorizing certificate, a data element or field of an identifying or authorizing certificate, a data file representing an image, data representing text, numbers, audio, and video.

French Abstract
L'invention concerne un procede de deroulement de donnees numeriques enroulees qui sont inutilisables tant qu'elles sont enroulees, caracterise par l'obtention d'une expression d'acceptation de la part d'un utilisateur, par la deduction d'une cle cryptographique a partir de l'expression d'acceptation et par le deroulement du paquet de donnees numeriques a l'aide de la cle cryptographique. L'expression d'acceptation est une expression saisie par un utilisateur en reponse aux informations fournies a cet utilisateur. Les informations et l'expression d'acceptation peuvent etre dans n'importe quel langage approprie. Les donnees numeriques comprennent, seul ou en combinaison, un logiciel, une cle cryptographique, un certificat d'identification, un certificat d'autorisation, un element de donnee ou champ d'un certificat d'identification ou d'autorisation, un fichier de donnees representant une image, des donnees sous forme textuelle, numerique, audio et visuelle.

12/5/7 (Item 7 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00424459 **Image available**
PAYMENT AND TRANSACTIONS IN ELECTRONIC COMMERCE SYSTEM
PAIEMENT ET TRANSACTIONS DANS UN SYSTEME DE COMMERCE ELECTRONIQUE
Patent Applicant/Assignee:
  CERTCO LLC,
Inventor(s):
  KRAVITZ David William
Patent and Priority Information (Country, Number, Date):
  Patent: WO 9814921 A1 19980409
  Application: WO 97US16930 19971001 (PCT/WO US9716930)
  Priority Application: US 96726434 19961004
Designated States: AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH HU IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZW GH KE LS MW SD SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN ML MR NE SN TD TG
Main International Patent Class: G07F-019/00
International Patent Class: G06F-17:60
Publication Language: English
Fulltext Availability:
  Detailed Description

Claims
Fulltext Word Count: 29178

English Abstract
A method of payment in an electronic payment system wherein a plurality of customers have accounts with an agent. A customer obtains an authenticated quote from a specific merchant, the quote including a specification of goods and a payment amount for those goods. The customer sends to the agent a single communication including a request for payment of the payment amount to the specific merchant and a unique identification of the customer. The agent issues to the customer an authenticated payment advice based only on the single communication and secret shared between the customer and the agent and status information which the agent knows about the merchant and/or the customer. The customer forwards a portion of the payment advice to the specific merchant. The specific merchant provides the goods to the customer in response to receiving the portion of the payment advice.

French Abstract
La presente invention concerne un procede de paiement dans un systeme de paiement electronique dans lequel une pluralite de clients ont des comptes chez un agent. Un client se procure une reference authentifiee chez un commercant particulier, la reference incluant une specification des marchandises et le prix a regler pour ces marchandises. Le client envoie une simple communication a l'agent comportant une demande de paiement du montant a payer au commercant considere et une identification unique dudit client. L'agent envoie au client un avis de paiement authentifie reposant sur la seule communication, sur le secret partage entre le client et l'agent, et sur l'information d'etat que l'agent connait concernant le commercant et/ou le client. Le client envoie une partie de l'avis de paiement au commercant particulier. Le commercant considere fournit les marchandises au client en reponse a la reception de la partie de l'avis de paiement.

12/5/8 (Item 8 from file: 349)

00358802 **Image available**
OFF-LINE COMPATIBLE ELECTRONIC CASH METHOD AND SYSTEM
PROCEDE ET SYSTEME AUTONOMES ET COMPATIBLES D'ECHANGE DE FONDS ELECTRONIQUES
Patent Applicant/Assignee:
KRAVITZ David W,
GEMMELL Peter S,
BRICKELL Ernest F,
Inventor(s):
KRAVITZ David W ,
GEMMELL Peter S,
BRICKELL Ernest F
Patent and Priority Information (Country, Number, Date):
Patent: WO 9641316 A2 19961219
Application: WO 96US10247 19960607 (PCT/WO US9610247)
Priority Application: US 95474033 19950607; US 95474035 19950607; US 95482356 19950607; US 95482685 19950607; US 95482686 19950607
Designated States: AL AM AT AU AZ BB BG BR BY CA CH CN CZ DE DK EE ES FI GB GE HU IS JP KE KG KP KR KZ LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK TJ TM TR TT UA UG US US US US US UZ VN KE LS MW SD SZ UG AM AZ BY KG KZ MD RU TJ TM AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN ML MR NE SN TD TG

Main International Patent Class: G07F-019/00
International Patent Class: G06F-17:60
Publication Language: English
Fulltext Availability:
  Detailed Description
  Claims
Fulltext Word Count: 18621

English Abstract
An off-line electronic cash system having an electronic coin, a bank B, a payee S, and a user U with an account at the bank B as well as a user password zu,i, has a method for performing an electronic cash transfer. An electronic coin is withdrawn from the bank B by the user U and an electronic record of the electronic coin is stored by the bank B. The coin is paid to the payee S by the user U. The payee S deposits the coin with the bank B. A determination is made that the coin is spent and the record of the coin is deleted by the bank B. A further deposit of the same coin after the record is deleted is determined. Additionally, a determination is made which user U originally withdrew the coin after deleting the record. To perform these operations, a key pair is generated by the user, including public and secret signature keys. The public signature key along with a user password zu,i and a withdrawal amount are sent to the bank B by the user U. In response, the bank B sends a coin to the user U signed by the secret key of the bank indicating the value of the coin and the public key of the user U. The payee S transmits a challenge counter to the user U prior to receiving the coin.

French Abstract
Ce systeme autonome d'echange de fonds electroniques comprend une monnaie electronique, une banque B, un beneficiaire S, et un utilisateur U possedant un compte aupres de la banque B ainsi qu'un mot de passe zu,i, un procede pour l'execution d'un transfert de fonds electroniques etant utilise avec ledit systeme. L'utilisateur U retire aupres de la banque B une monnaie electronique, de laquelle cette banque conserve un enregistrement electronique. La monnaie est payee par l'utilisateur U au beneficiaire S, lequel depose cette monnaie aupres de la banque B. Le fait que la monnaie a ete depensee est determine et la banque efface l'enregistrement de celle-ci, puis qu'un depot ulterieur de cette meme monnaie a ete effectue apres effacement de l'enregistrement. En outre, apres cet effacement, l'utilisateur U ayant retire originellement la monnaie est determine. Afin de realiser ces operations, l'utilisateur produit une paire de cles d'identification dont l'une est publique et l'autre secrete. L'utilisateur U envoie a la banque B la cle publique, en meme temps que son mot de passe zu,i, ainsi que le montant du retrait. En reponse, la banque B envoie a l'utilisateur U une monnaie qui porte la signature de la cle secrete de la banque indiquant la valeur de cette monnaie, ainsi que la signature de la cle publique de l'utilisateur U. Le beneficiaire S transmet un compteur d'identification a l'utilisateur U avant de recevoir la monnaie.
?

```
File 347:JAPIO Oct 1976-2003/Aug(Updated 031202)
         (c) 2003 JPO & JAPIO
File 350:Derwent WPIX 1963-2003/UD,UM &UP=200381
         (c) 2003  Thomson Derwent
? ds

Set     Items   Description
S1    2182527   MANUFACTUR??? ? OR PRODUCER? ? OR PRODUCING OR SUPPLIER? OR
               SUPPLYING
S2     241817   KEY? ? OR ALGORITHM? ? OR CIPHER? ? OR CYPHER? ?
S3       3929   PRIVATEKEY? OR (PRIVATE OR SECRET OR SYMMETRIC OR CONVENTI-
               ONAL)(1W)S2
S4      10398   (SERIAL OR UNIQUE)(2N)(IDENTIFIER? ? OR NUMBER? ? OR NUMER-
               IC?? ? OR NUMERAL? ? OR CODE OR CODES OR CODING?)
S5      16454   (UNIT OR MODULE OR COMPONENT OR DEVICE OR APPARAT? OR APP??
               ? OR EQUIPMENT OR APPLIANCE)(1W)(IDENTIFER? ? OR NUMBER? ? OR
               NUMERIC?? ? OR NUMERAL? OR CODE? ? OR CODING?)
S6          0   (SET()TOP OR SETTOP OR MEDIAPLAYER? OR (MULTIMEDIA OR MEDIA
               OR REAL OR FREE)()PLAYER? OR QUICKTIME OR FREEPLAYER?)(1W)(I-
               DENTIFER? ? OR NUMBER? ? OR NUMERIC?? ? OR NUMERAL? OR CODE? ?
               OR CODING?)
S7        116   (QUICK()TIME OR REALPLAYER? OR REALAUDIO OR REAL()AUDIO)(1-
               W)(IDENTIFER? ? OR NUMBER? ? OR NUMERIC?? ? OR NUMERAL? OR CO-
               DE? ? OR CODING?) OR UID OR UIDS
S8       5310   LICENS??? ? OR LICENC??? ?
S9        276   S8(7N)S2
S10        20   S9 AND S1
S11         2   S10 AND S3
S12         2   S10 AND S4:S7
S13         0   S11 AND S12
S14         4   S11:S12
S15         4   IDPAT (sorted in duplicate/non-duplicate order)
S16         4   IDPAT (primary/non-duplicate records only)
? t14/9/2-4

 14/9/2     (Item 2 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2003  Thomson Derwent. All rts. reserv.

014575609    **Image available**
WPI Acc No: 2002-396313/200243
XRPX Acc No: N02-310779
  Method for protection of computer software and computer- readable data
  against unauthorized use using a protection box that is used by an
  end-user for storage of license parameters relating to all his software
  from all  suppliers
Patent Assignee: WIBU SYSTEMS AG (WIBU-N)
Inventor: BUCHHEIT M; WINZENRIED O
Number of Countries: 027  Number of Patents: 003
Patent Family:
Patent No     Kind   Date    Applicat No    Kind   Date     Week
EP 1184771     A1  20020306  EP 2000118372   A   20000824  200243  B
US 20020031222  A1  20020314  US 2001938023   A   20010822  200244
JP 2002116839  A   20020419  JP 2001254539   A   20010824  200244

Priority Applications (No Type Date): EP 2000118372 A 20000824
Patent Details:
Patent No  Kind Lan Pg   Main IPC    Filing Notes
EP 1184771    A1 G  18 G06F-001/00
   Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT
   LI LT LU LV MC MK NL PT RO SE SI
```

US 20020031222 A1 H04N-007/167
JP 2002116839 A 11 G06F-001/00

Abstract (Basic): EP 1184771 A1

NOVELTY - Method comprises encoding of the software by a license provider using license parameters, recording of software, encoded license parameter transfer from provider to license taker and automatic encoding of the software using the license parameters while the software is being used by the license taker.

DETAILED DESCRIPTION - Software encoding is initialized with a freely chosen **secret** Firm **Key** (FK). Encoding of the transmitted **license** parameters is undertaken using a **Private** Serial **Key** (SK). Decoding of the software or data is initiated using the selected Firm Key. An INDEPENDENT CLAIM is made for a device for **producing** a random secret **private** serial **key** for encoding the **license** parameters before they are transferred from the license provider to the license taker. Ideally the device is connected to the computer of the license taker.

USE - Protection of computer software and or data using encryption.

ADVANTAGE - The invention prevents unauthorized copying and allows storage or recording of a large number of independent license parameters for a large number of software products provided by independent software providers.

DESCRIPTION OF DRAWING(S) - (Drawing includes non-English language text). Figure shows a method for protection of computer software or computer readable data, including billing for its use, using a hardware add-on designed as a protection device.

license taker or end-user (2)
license or software providers (1a-c)
protection device or box. (3)
pp; 18 DwgNo 1/8

Title Terms: METHOD; PROTECT; COMPUTER; SOFTWARE; COMPUTER; READ; DATA; UNAUTHORISED; PROTECT; BOX; END; USER; STORAGE; LICENCE; PARAMETER; RELATED; SOFTWARE; SUPPLY
Derwent Class: T01
International Patent Class (Main): G06F-001/00; H04N-007/167
International Patent Class (Additional): G06F-012/14; G06F-017/60
File Segment: EPI
Manual Codes (EPI/S-X): T01-D01; T01-H01C2; T01-J12C; T01-J20B2A

14/9/3 (Item 3 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014136736 **Image available**
WPI Acc No: 2001-620947/200172
XRPX Acc No: N01-463317

Goods authentication card for goods sale, displays authorization number with product type number , manufacturer **'s** serial number **and authentication** key **for every** licensed **good print in card board**

Patent Assignee: SPORTS STATION KK (SPOR-N)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 2001222734	A	20010817	JP 200034675	A	20000214	200172	B

Priority Applications (No Type Date): JP 200034675 A 20000214
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes

JP 2001222734 A 6 G07D-007/20

Abstract (Basic): JP 2001222734 A
NOVELTY - A goods authorization card (1) displays a authorization number with product type **number** (6), a **serial number** (7) which shows the **manufacturer** 's **serial number** of the product and an authentication **key** (8) for every **licensed** good in a card board (2).
DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for goods authorization card authentication method.
USE - For identifying genuiness of goods during goods sale.
ADVANTAGE - A goods authorization card performs guaranteed management of goods and prevents counterfeiting of goods.
DESCRIPTION OF DRAWING(S) - The figure shows the top view of the goods authorization card. (Drawing includes non-English language text).

Goods authorization card (1)
Card board (2)
Product type number (6)
Serial number (7)
Authentication key (8)
pp; 6 DwgNo 1/2

Title Terms: GOODS; AUTHENTICITY; CARD; GOODS; SALE; DISPLAY; NUMBER; PRODUCT; TYPE; NUMBER; **MANUFACTURE** ; SERIAL; NUMBER; AUTHENTICITY; KEY; PRINT; CARD; BOARD
Derwent Class: P85; T05
International Patent Class (Main): G07D-007/20
International Patent Class (Additional): G07F-007/08; G09F-001/02; G09F-003/02
File Segment: EPI; EngPI
Manual Codes (EPI/S-X): T05-H02C

14/9/4 (Item 4 from file: 350)
DIALOG(R)File 350:Derwent WPIX

010525087 **Image available**
WPI Acc No: 1996-022040/199603
XRPX Acc No: N96-018294
Security enhancement method for distributed software - involves providing private key , **application writer's** license **and software in code with message digest and** supplying **to user computed from code using** private key
Patent Assignee: SUN MICROSYSTEMS INC (SUNM)
Inventor: CHANG S; GOSLING J
Number of Countries: 007 Number of Patents: 004
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 686906	A2	19951213	EP 95303720	A	19950531	199603	B
JP 8166879	A	19960625	JP 95144507	A	19950612	199635	
EP 686906	A3	19970806	EP 95303720	A	19950531	199743	
US 5724425	A	19980303	US 94258244	A	19940610	199816	

Priority Applications (No Type Date): US 94258244 A 19940610
Cited Patents: No-SR.Pub; 2.Jnl.Ref; EP 328232
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 686906	A2	E	15	G06F-001/00	
Designated States (Regional): DE FR GB NL SE					
JP 8166879	A		16	G06F-009/06	

US 5724425 A 37 H04L-009/00
EP 686906 A3 G06F-001/00

Abstract (Basic): EP 686906 A

The enhancement method involves providing a computer (10) and a **private key** . An application writer's **license** is provided which contains a public **key** . Software is also provided. The **private key** , writer's **license** and software are supplied to a compiler by the computer. The software is compiled into binary code and a message digest is computed for the code.

The computer further encrypts the message digest using the **private key** . The encrypted message digest comprises an application writer's digital signature. The computer generates a software passport comprising the application writer's digital signature and the application writer's license. The software passport and the binary code is distributed to a user.

ADVANTAGE - Provides method and apparatus for authenticating software distributed by **manufacturer** . Ensures software contains only original **manufacturers** code without any tampering.

Dwg.1/6

Abstract (Equivalent): US 5724425 A

The enhancement method involves providing a computer (10) and a **private key** . An application writer's **license** is provided which contains a public **key** . Software is also provided. The **private key** , writer's **license** and software are supplied to a compiler by the computer. The software is compiled into binary code and a message digest is computed for the code.

The computer further encrypts the message digest using the **private key** . The encrypted message digest comprises an application writer's digital signature. The computer generates a software passport comprising the application writer's digital signature and the application writer's license. The software passport and the binary code is distributed to a user.

ADVANTAGE - Provides method and apparatus for authenticating software distributed by **manufacturer** . Ensures software contains only original **manufacturers** code without any tampering.

Dwg.1/6b

Title Terms: SECURE; ENHANCE; METHOD; DISTRIBUTE; SOFTWARE; PRIVATE; KEY; APPLY; WRITING; LICENCE; SOFTWARE; CODE; MESSAGE; DIGEST; SUPPLY; USER; COMPUTATION; CODE; PRIVATE; KEY

Derwent Class: T01

International Patent Class (Main): G06F-001/00; G06F-009/06; H04L-009/00

International Patent Class (Additional): H04L-009/30; H04L-009/32

File Segment: EPI

Manual Codes (EPI/S-X): T01-J20X

```
File   9:Business & Industry(R) Jul/1994-2003/Dec 22
         (c) 2003 Resp. DB Svcs.
File  16:Gale Group PROMT(R) 1990-2003/Dec 24
         (c) 2003 The Gale Group
File  47:Gale Group Magazine DB(TM) 1959-2003/Dec 19
         (c) 2003 The Gale group
File 148:Gale Group Trade & Industry DB 1976-2003/Dec 22
         (c)2003 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 275:Gale Group Computer DB(TM) 1983-2003/Dec 23
         (c) 2003 The Gale Group
File 570:Gale Group MARS(R) 1984-2003/Dec 23
         (c) 2003 The Gale Group
File 621:Gale Group New Prod.Annou.(R) 1985-2003/Dec 22
         (c) 2003 The Gale Group
File 636:Gale Group Newsletter DB(TM) 1987-2003/Dec 23
         (c) 2003 The Gale Group
File 649:Gale Group Newswire ASAP(TM) 2003/Dec 19
         (c) 2003 The Gale Group
? ds

Set     Items   Description
S1   13479783   MANUFACTUR??? ? OR PRODUCER? ? OR PRODUCING OR SUPPLIER? OR
             SUPPLYING
S2    3757524   KEY? ? OR ALGORITHM? ? OR CIPHER? ? OR CYPHER? ?
S3      11810   PRIVATEKEY? OR (PRIVATE OR SECRET OR SYMMETRIC OR CONVENTI-
             ONAL)(1W)S2
S4      50390   (SERIAL OR UNIQUE)(2N)(IDENTIFIER? ? OR NUMBER? ? OR NUMER-
             IC?? ? OR NUMERAL? ? OR CODE OR CODES OR CODING?)
S5      12650   (UNIT OR MODULE OR COMPONENT OR DEVICE OR APPARAT? OR APP??
              ? OR EQUIPMENT OR APPLIANCE)(1W)(IDENTIFER? ? OR NUMBER? ? OR
              NUMERIC?? ? OR NUMERAL? OR CODE? ? OR CODING?)
S6        386   (SET()TOP OR SETTOP OR MEDIAPLAYER? OR (MULTIMEDIA OR MEDIA
              OR REAL OR FREE)()PLAYER? OR QUICKTIME OR FREEPLAYER?)(1W)(I-
             DENTIFER? ? OR NUMBER? ? OR NUMERIC?? ? OR NUMERAL? OR CODE? ?
              OR CODING?)
S7        824   (QUICK()TIME OR REALPLAYER? OR REALAUDIO OR REAL()AUDIO)(1-
             W)(IDENTIFER? ? OR NUMBER? ? OR NUMERIC?? ? OR NUMERAL? OR CO-
             DE? ? OR CODING?) OR UID OR UIDS
S8    2469277   LICENS??? ? OR LICENC??? ?
S9      34868   S8(7N)S2
S10      3132   S9(S)S1
S11         2   S10(S)S3
S12        10   S10(S)S4:S7
S13         0   S11(S)S12
S14        12   S11:S12
S15         7   S14/2000:2003
S16         5   S14 NOT S15
S17         4   RD (unique items)
? t17/3,k/2,4

 17/3,K/2     (Item 2 from file: 16)
DIALOG(R)File  16:Gale Group PROMT(R)
(c) 2003 The Gale Group. All rts. reserv.

03696254    Supplier Number: 45231313
US Telecommunications Network Security and Reliability Equipment and
  Service Markets: Network Fulfillment Vital to the Information Industry
Research Studies-Frost & Sullivan, p1
```

Jan, 1995
Language: English Record Type: Abstract
Document Type: Magazine/Journal; Trade

ABSTRACT:
...sophisticated. For instance, growing attention is being directed toward encryption algorithms such as the public/ **private key algorithms** that RSA Company 1licenses for use by **manufacturers** . A major trend in network security involves bringing the equipment and services into the cost...

...fees from their customers, or as a way of differentiating their services from competition. PBX **manufacturers** also have the opportunity to obtain higher revenues or to gain a competitive edge with...

17/3,K/4 (Item 1 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)

02977713 Supplier Number: 46068964 (USE FORMAT 7 FOR FULLTEXT)
SCIENTIFIC-ATLANTA: PowerKEY conditional access system using RSA 'Public Key' encryption techniques
M2 Presswire, pN/A
Jan 16, 1996
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 996

... to Scientific-Atlanta is the first that RSA has granted to a set-top terminal **manufacturer** of its widely adopted, patented technique for private messaging and digital signature authentication. The agreement provides for the **licensing** of RSA technology, including the **algorithms** that enable RSA's public key- **private key** cryptography. No other terms of the agreement were disclosed.
With the PowerKEY system, Scientific-Atlanta...
?

File 348:EUROPEAN PATENTS 1978-2003/Dec W02
(c) 2003 European Patent Office
File 349:PCT FULLTEXT 1979-2002/UB=20031218,UT=20031211
(c) 2003 WIPO/Univentio
? ds

Set	Items	Description
S1	839371	MANUFACTUR??? ? OR PRODUCER? ? OR PRODUCING OR SUPPLIER? OR SUPPLYING
S2	221434	KEY? ? OR ALGORITHM? ? OR CIPHER? ? OR CYPHER? ?
S3	8797	PRIVATEKEY? OR (PRIVATE OR SECRET OR SYMMETRIC OR CONVENTIONAL)(1W)S2
S4	53348	(SERIAL OR UNIQUE)(2N)(IDENTIFIER? ? OR NUMBER? ? OR NUMERIC?? ? OR NUMERAL? ? OR CODE OR CODES OR CODING?)
S5	19637	(UNIT OR MODULE OR COMPONENT OR DEVICE OR APPARAT? OR APP?? ? OR EQUIPMENT OR APPLIANCE)(1W)(IDENTIFER? ? OR NUMBER? ? OR NUMERIC?? ? OR NUMERAL? OR CODE? ? OR CODING?)
S6	33	(SET()TOP OR SETTOP OR MEDIAPLAYER? OR (MULTIMEDIA OR MEDIA OR REAL OR FREE)()PLAYER? OR QUICKTIME OR FREEPLAYER?)(1W)(IDENTIFER? ? OR NUMBER? ? OR NUMERIC?? ? OR NUMERAL? OR CODE? ? OR CODING?)
S7	3129	(QUICK()TIME OR REALPLAYER? OR REALAUDIO OR REAL()AUDIO)(1W)(IDENTIFER? ? OR NUMBER? ? OR NUMERIC?? ? OR NUMERAL? OR CODE? ? OR CODING?) OR UID OR UIDS
S8	19354	LICENS??? ? OR LICENC??? ?
S9	637	S8(7N)S2
S10	62	S9(25N)S1
S11	18	S10(25N)S3
S12	3	S10(25N)S4:S7
S13	0	S11(S)S12
S14	21	S11:S12
S15	21	IDPAT (sorted in duplicate/non-duplicate order)
S16	20	IDPAT (primary/non-duplicate records only)

? t16/5,k/1-2,4-5,7-9

16/5,K/1 (Item 1 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01660694
Management of different configurations and different levels of functionalities in equipment for telecommunications networks
Verwaltung verschiedener Konfigurationen und verschiedener Funktionalitatsebenen in Telekommunikationsnetzwerkgeraten
Administration de differentes configurations et de differents niveaux de fonctionnalite dans un equipement pour reseaux de telecommunication
PATENT ASSIGNEE:
ALCATEL, (201876), 54, rue La Boetie, 75008 Paris, (FR), (Applicant designated States: all)
INVENTOR:
Fumagalli, Aurelio, Via Roma, 33, 23876 Monticello Brianza (Lecco), (IT)
Perego, Maria Adele, Via della Fontana, 5, 20045 Besana Brianza (Milano), (IT)
Sedini, Augusto, Via Cosmi, 29, 20060 Trezzano Rosa (Milano), (IT)
LEGAL REPRESENTATIVE:
Lamoureux, Bernard (83291), Compagnie Financiere Alcatel Departement de Propriete Industrielle, 5, rue Noel Pons, 92734 Nanterre Cedex, (FR)
PATENT (CC, No, Kind, Date): EP 1365608 A1 031126 (Basic)
APPLICATION (CC, No, Date): EP 2003291016 030425;
PRIORITY (CC, No, Date): IT 20MI21017 020514

DESIGNATED STATES: AT; BE; BG; CH; CY; CZ; DE; DK; EE; ES; FI; FR; GB; GR; HU; IE; IT; LI; LU; MC; NL; PT; RO; SE; SI; SK; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK
INTERNATIONAL PATENT CLASS: H04Q-007/32; G06F-001/00

ABSTRACT EP 1365608 A1
A method for managing different configurations and different levels of functionalities in equipment for telecommunications networks is described. The method calls for the following phases: definition of one or more licences, each licence being associated with corresponding configurations and/or levels of functions; provision of a semi-permanent equipment memory; provision of a software program to be loaded in the equipment to enable its normal operation; and preset of the semi-permanent equipment memory by storing indicative information referred to a licence so that the equipment software program will learn the licence on the basis of the information that is stored and make only those functions that are associated with the licence available
ABSTRACT WORD COUNT: 111
NOTE:
Figure number on first page: 1

LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 031126 A1 Published application with search report
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200348	416
SPEC A	(English)	200348	2656
Total word count - document A			3072
Total word count - document B			0
Total word count - documents A + B			3072

...SPECIFICATION installed.
3. On receiving the application for an up-date of the licence, the equipment **manufacturer** will define the code of the new **licence** and will develop an authentication **key** , on the basis of the information received about the **equipment** (identification **code** of the memory of the equipment). The following information is then notified to the owner ...

...basis of the configurations and of the functionalities it covers) requested by the owner (equipment **manufacturer**). The **equipment code** remains unchanged;
15: generation of a new **key** for enabling the requested **licence** (equipment **manufacturer**);
16: supply of the codes (licence codes and, if required, also the **equipment code** , which in any case is unchanged) and of the key to the owner of the...

...CLAIMS licence is required to be up-dated; notification of the licence code and of the **equipment code** to the **manufacturer** ; development of a new licence code on the basis of the new licence applied for by the owner; generation of a new **key** for enabling the **licence** applied for; provision of the licence code and, if required, also of the **equipment code** and of the key to the equipment owner; enabling of the new codes for the...

16/5,K/2 (Item 2 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01643250

Information recording medium, recording apparatus, and reproduction apparatus

Informationsaufzeichnungsmedium, Aufzeichnungsgerat, und Wiedergabegerat

Support d'enregistrement d'information, appareil d'enregistrement, et appareil de reproduction

PATENT ASSIGNEE:
MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD., (216883), 1006, Oaza-Kadoma, Kadoma-shi, Osaka 571-8501, (JP), (Applicant designated States: all)
INVENTOR:
Yumiba, Takashi, 13-7, Yamateminami 2-chome, Kyotanabe-shi, Kyoto 610-0354, (JP)
Yamaoka, Masaru, 25-3, Midocho, Kadoma-shi, Osaka 571-0064, (JP)
Nagai, Takahiro, 23-10-407, Takadono 6-chome, Asahi-ku, Osaka-shi, Osaka 535-0031, (JP)
LEGAL REPRESENTATIVE:
Balsters, Robert et al (83703), Novagraaf International S.A. 25, avenue du Pailly, 1220 Les Avanchets - Geneva, (CH)

PATENT (CC, No, Kind, Date): EP 1353330 A1 031015 (Basic)
APPLICATION (CC, No, Date): EP 2003007479 030407;
PRIORITY (CC, No, Date): JP 2002106170 020409
DESIGNATED STATES: AT; BE; BG; CH; CY; CZ; DE; DK; EE; ES; FI; FR; GB; GR; HU; IE; IT; LI; LU; MC; NL; PT; RO; SE; SI; SK; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO
INTERNATIONAL PATENT CLASS: G11B-020/00

ABSTRACT EP 1353330 A1

An information recording medium for recording main information and auxiliary information is provided. The auxiliary information is recorded on the information recording medium in a manner that edge positions of the pits or the recording marks indicating the main information are shifted either in a phase advancing direction or in a phase delaying direction along the track direction. A predetermined frequency is used to determine whether the edge position is shifted in the phase advancing direction or in the phase delaying direction in order to record the auxiliary information. The predetermined frequency is substantially consistently lower than 1/2 of a reference frequency of a recording clock for creating the pits or the recording marks and is higher than a response frequency of a PLL for generating a reproduction clock for reproducing the main information.

ABSTRACT WORD COUNT: 135
NOTE:
Figure number on first page: 1

LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 031015 A1 Published application with search report
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200342	1275
SPEC A	(English)	200342	9444
Total word count - document A			10719
Total word count - document B			0
Total word count - documents A + B			10719

...SPECIFICATION region accessible for the user. The master key, which is the most important of the **private keys** , is provided only to **licensed** , authorized **manufacturers** . The disc **key** and the title key, which are required for each DVD and each title, respectively, are...

16/5,K/4 **(Item 4 from file: 348)**
DIALOG(R)File 348:EUROPEAN PATENTS

01399333
Method and device for protection of computer software and/or computer-readable data
Verfahren zum Schutz von Computer-Software und/oder computerlesbaren Daten sowie Schutzgerat
Methode et dispositif de protection de logiciels d'ordinateur et/ou donnees lisibles par un ordinateur
PATENT ASSIGNEE:
Wibu-Systems AG, (3098800), Ruppurrer Strasse 52-54, 76137 Karlsruhe, (DE), (Applicant designated States: all)
INVENTOR:
Buchheit, Marcellus, Kronenstrasse 30, 76133 Karlsruhe, (DE)
Winzenried, Oliver, Ruppurrer Strasse 52, 76137 Karlsruhe, (DE)
LEGAL REPRESENTATIVE:
Durm, Frank, Dipl.-Ing. et al (55383), Patentanwalte, Durm & Durm, Moltkestrasse 45, 76133 Karlsruhe, (DE)
PATENT (CC, No, Kind, Date): EP 1184771 A1 020306 (Basic)
APPLICATION (CC, No, Date): EP 2000118372 000824;
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: G06F-001/00

ABSTRACT EP 1184771 A1 (Translated)
Method for protection of computer software and computer- readable data against unauthorized use using a protection box that is used by an end-user for storage of license parameters relating to all his software from all supp

Method comprises encoding of the software by a license provider using license parameters, recording of software, encoded license parameter transfer from provider to license taker and automatic encoding of the software using the license parameters while the software is being used by the license taker.

Software encoding is initialized with a freely chosen **secret** Firm **Key** (FK). Encoding of the transmitted **license** parameters is undertaken using a **Private** Serial **Key** (SK). Decoding of the software or data is initiated using the selected Firm Key. An Independent claim is made for a device for **producing** a random secret **private** serial **key** for encoding the **license** parameters before they are transferred from the license provider to the license taker. Ideally the device is connected to the computer of the license taker.
TRANSLATED ABSTRACT WORD COUNT: 165
ABSTRACT EP 1184771 A1
Ein Verfahren zum Schutz von Computer-Software und/oder computerlesbaren Daten gegen unberechtigte Nutzung umfasst die Verschlusselung der Software durch den Lizenzgeber in Abhangigkeit von Lizenzparametern, das Speichern der Software beim Lizenznehmer, die verschlusselte Ubertragung der Lizenzparameter vom Lizenzgeber an den Lizenznehmer sowie die automatische Entschlusselung der Software in Abhangigkeit der eingespeicherten Lizenzparameter wahrend der Nutzung der Software durch den Lizenznehmer.

Die Verschlusselung der Software wird initialisiert in Abhangigkeit eines vom Lizenzgeber frei gewahlten geheimen Firm Key (FK). Die Verschlusselung der Ubertragung der Lizenzparameter erfolgt in

Abhangigkeit eines geheimen Private Serial Key (SK). Die Entschlusselung der Software bzw. Daten wird initialisiert in Abhangigkeit des vom Lizenzgeber gewahlten Firm Key (FK).

Das Verfahren erlaubt einen besonders sicheren Kopierschutz und ermoglicht das Speichern einer Vielzahl voneinander unabhangiger Lizenzparameter verschiedener Lizenzgeber. Bevorzugt findet ein Schutzgerat (3) Verwendung, das an den Computer (2) des Lizenznehmers angeschlossen ist und einen Speicher (6) mit mehreren Speicherbereichen (6a, 6b, 6c) fur die Einspeicherung von Lizenzparametern verschiedener Lizenzgeber umfasst.

ABSTRACT WORD COUNT: 160

NOTE:

Figure number on first page: 1

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application: 020306 A1 Published application with search report

Examination: 020306 A1 Date of request for examination: 20010313

LANGUAGE (Publication,Procedural,Application): German; German; German

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(German)	200210	585
SPEC A	(German)	200210	3472
Total word count - document A			4057
Total word count - document B			0
Total word count - documents A + B			4057

...ABSTRACT is being used by the license taker.

Software encoding is initialized with a freely chosen **secret** Firm **Key** (FK). Encoding of the transmitted **license** parameters is undertaken using a **Private** Serial **Key** (SK). Decoding of the software or data is initiated using the selected Firm Key. An Independent claim is made for a device for **producing** a random secret **private** serial **key** for encoding the **license** parameters before they are transferred from the license provider to the license taker. Ideally the...

16/5,K/5 (Item 5 from file: 348)

DIALOG(R)File 348:EUROPEAN PATENTS

00968334

Information recording apparatus, information reproducing apparatus, and information distribution system

Informationsaufzeichnungs- und -wiedergabegerat sowie Informationsverteilungssystem

Appareil d'enregistrement d'informations, appareil de reproduction d'informations, et systeme de distribution d'informations

PATENT ASSIGNEE:

KABUSHIKI KAISHA TOSHIBA, (213137), 72, Horikawa-cho, Saiwai-ku, Kawasaki-shi, Kanagawa 210-8520, (JP), (Applicant designated States: all)

INVENTOR:

Kambayashi, Toru, c/o Kabushiki Kaisha Toshiba, Intell. Prop. Div., 1-1 Shibaura 1-chome, Minato-ku, Tokyo 105-8001, (JP)

Akiyama, Koichiro, c/o Kabushiki Kaisha Toshiba, Intell. Prop. Div., 1-1 Shibaura 1-chome, Minato-ku, Tokyo 105-8001, (JP)

Tsujimoto, Shuichi, c/o Kabushiki Kaisha Toshiba, Intell. Prop. Div., 1-1 Shibaura 1-chome, Minato-ku, Tokyo 105-8001, (JP)

Sumita, Kazuo, c/o Kabushiki Kaisha Toshiba, Intell. Prop. Div., 1-1 Shibaura 1-chome, Minato-ku, Tokyo 105-8001, (JP)

Hirakawa, Hideki, c/o Kabushiki Kaisha Toshiba, Intell. Prop. Div., 1-1 Shibaura 1-chome, Minato-ku, Tokyo 105-8001, (JP)
Sugaya, Toshihiro, c/o Kabushiki Kaisha Toshiba, Intell. Prop. Div., 1-1 Shibaura 1-chome, Minato-ku, Tokyo 105-8001, (JP)
LEGAL REPRESENTATIVE:
Henkel, Feiler, Hanzel (100401), Mohlstrasse 37, 81675 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 878796 A2 981118 (Basic)
EP 878796 A3 000524
APPLICATION (CC, No, Date): EP 98108638 980512;
PRIORITY (CC, No, Date): JP 97122511 970513; JP 9816618 980129
DESIGNATED STATES: DE; NL
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: G11B-020/00; G06F-001/00; H04L-009/00

ABSTRACT EP 878796 A2
An information recording apparatus comprises an encryption section (7) encrypting contents information and also a license condition referred to to limit use of the contents information and a decoding key for decoding the encrypted contents information to generate license information, and a recording section (8) recording the encrypted contents information and the generated license information on a recording medium. An information reproducing apparatus comprises a decoder unit (103) decoding the license information recorded on the recording medium using a second decoding key for decoding the license information and deciding on the basis of the license condition contained in the decoded license information whether the contents information can be used. If it is decided that the contents information can be used, the encrypted contents information recorded on the recording medium is decoded using the first decoding key contained in the decoded license information.
ABSTRACT WORD COUNT: 143
NOTE:
Figure number on first page: 1+8

LEGAL STATUS (Type, Pub Date, Kind, Text):
Search Report: 000524 A3 Separate publication of the search report
Application: 981118 A2 Published application (A1with Search Report ;A2without Search Report)
Examination: 030507 A2 Date of dispatch of the first examination report: 20030321
Examination: 981118 A2 Date of filing of request for examination: 980609
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	9847	2220
SPEC A	(English)	9847	55951
Total word count - document A			58171
Total word count - document B			0
Total word count - documents A + B			58171

...SPECIFICATION decides that the contents information can be used.
The key generation section generates a public **key** used to encrypt the **license** information and a **secret key** for decoding the **license** information, the **secret key** corresponding to the public key, the apparatus further comprises update request section for, when the decision section decides that the contents information cannot be used, **supplying** at least newly designated **license** condition and a public **key** newly generated by the **key** generation section to request update of the **license** information, and the license information updated in response to the license information update request from...

16/5,K/7 **(Item 7 from file: 348)**
DIALOG(R)File 348:EUROPEAN PATENTS

00558804
MANAGEMENT INTERFACE AND FORMAT FOR LICENSE MANAGEMENT SYSTEM
VERWALTUNGSSSCHNITTSTELLE UND FORMAT FUR LIZENZVERWALTUNGSSYSTEM
INTERFACE DE GESTION ET FORMAT POUR SYSTEME DE GESTION DE LICENCES
PATENT ASSIGNEE:
DIGITAL EQUIPMENT CORPORATION, (313080), 146 Main Street, Maynard, MA 01754, (US), (applicant designated states: DE;FR;GB;IT)
INVENTOR:
WYMAN, Robert, Mark, 410 Second Avenue, South 108, Kirkland, WA 98033, (US)
LEGAL REPRESENTATIVE:
Goodman, Christopher et al (31122), Eric Potter Clarkson, Park View House, 58 The Ropewalk, Nottingham NG1 5DD, (GB)
PATENT (CC, No, Kind, Date): EP 538453 A1 930428 (Basic)
EP 538453 B1 990203
WO 9220022 921112
APPLICATION (CC, No, Date): EP 92912052 920506; WO 92US3812 920506
PRIORITY (CC, No, Date): US 697652 910508; US 723456 910628; US 722840 910628; US 723457 910628
DESIGNATED STATES: DE; FR; GB; IT
INTERNATIONAL PATENT CLASS: G06F-001/00; G06F-017/60;
CITED PATENTS (WO A): EP 332304 A; EP 332304 A; EP 332304 A
CITED REFERENCES (WO A):
IBM TECHNICAL DISCLOSURE BULLETIN. vol. 31, no. 8, 1 January 1989, NEW YORK US pages 195 - 198; 'METHOD FOR MANAGING CLIENT/SERVER RELATIONSHIP IN THE AIX OPERATING SYSTEM';
NOTE:
No A-document published by EPO
LEGAL STATUS (Type, Pub Date, Kind, Text):
Oppn None: 20000119 B1 No opposition filed: 19991104
Application: 930428 A1 Published application (A1with Search Report ;A2without Search Report)
Examination: 930623 A1 Date of filing of request for examination: 930423
Examination: 970416 A1 Date of despatch of first examination report: 970305
Change: 980422 A1 International patent classification (change)
Change: 980422 A1 Obligatory supplementary classification (change)
Change: 980527 A1 Representative (change)
Grant: 990203 B1 Granted patent
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	9905	867
CLAIMS B	(German)	9905	888
CLAIMS B	(French)	9905	998
SPEC B	(English)	9905	24869
Total word count - document A			0
Total word count - document B			27622
Total word count - documents A + B			27622

...SPECIFICATION who have been registered as authorized license issuers and provided with an appropriate public and **private key** pair. The key registration identifies the public **key** which is to be used by conforming **license** managers 10 in evaluating signatures 53 created by

the named issuer 25 or **producer** 28. A key registration syntax diagram is shown in Figure 22. Key-owner-name provides...

16/5,K/8 (Item 8 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01045289 **Image available**
INFORMATION RECORDING MEDIUM, USAGE MANAGEMENT METHOD, AND USAGE MANAGEMENT APPARATUS
SUPPORT D'ENREGISTREMENT D'INFORMATIONS, PROCEDE ET APPAREIL DE GESTION DE L'UTILISATION
Patent Applicant/Assignee:
MATSUSHITA ELECTRIC INDUSTRIAL CO LTD, 1006, Oazakadoma, Kadoma-shi, Osaka 571-8501, JP, JP (Residence), JP (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
YAMAOKA Masaru, 25-3, Mido-cho, Kadoma-shi, Osaka 571-0064, JP, JP (Residence), JP (Nationality), (Designated only for: US)
YUMIBA Takashi, 2-13-7, Yamate-minami, Kyotanabe-shi, Kyoto 611-0354, JP, JP (Residence), JP (Nationality), (Designated only for: US)
NAGAI Takahiro, 6-23-10-407, Takadono, Asahi-ku, Osaka-shi, Osaka 535-0031, JP, JP (Residence), JP (Nationality), (Designated only for: US)
ISHIHARA Hideshi, 1-10-120, Ikuno, Katano-shi, Osaka 576-0054, JP, JP (Residence), JP (Nationality), (Designated only for: US)
Legal Representative:
NAKAJIMA Shiro (agent), 6F, Yodogawa 5-Bankan, 2-1, Toyosaki 3-chome, Osaka-shi, Osaka 531-0072, JP,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200375273 A2 20030912 (WO 0375273)
Application: WO 2003JP2697 20030307 (PCT/WO JP0302697)
Priority Application: JP 200261433 20020307
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NI NO NZ OM PH PL PT RO RU SC SD SE SG SK SL TJ TM TN TR TT TZ UA UG US UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT RO SE SI SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: G11B-020/00
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 19765
English Abstract
A digital work and copyright management information for the digital work are recorded on an information recording medium by altering a shape, a position or a pattern of recording mark edges of the digital work. Alternatively, a decryption key for the right management information is recorded on an information recording medium on which the copyright management information has been recorded encrypted, by altering the recording mark edges of the copyright management information. Alternatively, a check code for the copyright management information is recorded on the information recording medium by altering the recording mark edges. The check code is checked when the copyright management

information is read, thus detecting illegal use of the copyright management information.

French Abstract
L'invention concerne une oeuvre numerique et des informations de gestion du droit d'auteur de l'oeuvre numerique qui sont enregistrees sur un support d'enregistrement d'informations par modification d'une forme, d'une position ou d'un motif des bords de marques d'enregistrement de l'oeuvre numerique. Dans un mode de realisation, on enregistre une cle de dechiffrement des informations de gestion correctes sur un support d'enregistrement d'informations sur lequel on a enregistre les informations chiffrees de gestion du droit d'auteur, en modifiant les bords de marques d'enregistrement des informations de gestion du droit d'auteur. Dans un autre mode de realisation, on enregistre, sur le support d'enregistrement d'informations, un code de verification des informations de gestion du droit d'auteur en modifiant les bords des marques d'enregistrement. Le code de verification est verifie lorsque les informations de gestion du droit d'auteur sont lues, l'utilisation illegale des informations de gestion du droit d'auteur etant ainsi detectee.

Legal Status (Type, Date, Text)
Publication 20030912 A2 Without international search report and to be republished upon receipt of that report.
Examination 20031120 Request for preliminary examination prior to end of 19th month from priority date

Fulltext Availability:
Detailed Description

Detailed Description
... a user
information area that is accessible by a user.
The most important of the **secret keys** , the master key, is known only to **manufacturers** who have a legitimate **license** .

The disc **key** and the title **key** , which are unique to each DVD and each title respectively, are scrambled based on the...

16/5,K/9 (Item 9 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01033091 **Image available**
GAMING SYSTEM LICENSE MANAGEMENT
GESTION DE LICENCE DE SYSTEME DE JEU
Patent Applicant/Assignee:
IGT, 9295 Prototype Drive, Reno, NV 89511, US, US (Residence), US (Nationality)
Inventor(s):
OBERBERGER Mike, 4591 Lynnfield Ct., Reno, NV 89509, US,
Legal Representative:
HIRSCH Martin J (agent), Marshall, Gerstein & Borun, 6300 Sears Tower, 233 South Wacker Drive, Chicago, IL 60606, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200363101 A1 20030731 (WO 0363101)
Application: WO 2002US9238 20020326 (PCT/WO US0209238)
Priority Application: US 200250747 20020116
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP

KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO
RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG US UZ VN YU ZA ZM ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: G07F-017/32
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 14737

English Abstract
A gaming system may include a first gaming unit, a second gaming unit, and a monitoring apparatus operatively coupled to the first and second gaming unit. The monitoring apparatus may include a display terminal and a monitoring apparatus controller operatively coupled to the display terminal. The monitoring apparatus controller may comprise a processor and a memory having encrypted license data representing a license parameter and a corresponding license parameter value stored therein, and may be programmed to determine if the encrypted license data is authentic and may be programmed to determine if a configuration of the gaming system is in compliance with the license parameter value of the license parameter.

French Abstract
L'invention concerne un systeme de jeu comprenant une premiere unite de jeu, une seconde unite de jeu et un appareil de surveillance couple, de facon operationnelle, a ces deux unites. L'appareil de surveillance comprend un terminal ecran et une unite de commande couplee, de facon operationnelle, au terminal ecran. L'unite de commande de l'appareil de surveillance comprend un processeur et une memoire contenant des donnees codees de licence representant un parametre de licence et une valeur de ce parametre stockee dedans, ce processeur etant programme afin de determiner si les donnees codees de licence sont authentiques et si une configuration du systeme de jeu correspond a la valeur du parametre de licence.

Legal Status (Type, Date, Text)
Publication 20030731 A1 With international search report.
Examination 20031023 Request for preliminary examination prior to end of 19th month from priority date

Fulltext Availability:
Detailed Description
Detailed Description
... encrypting and decrypting. Next, a license signature is derived at block 210 by applying a
private key from a public- **private key** pair to the first hash value. The
license signature, generated when the **licensor** 's **private key** is applied to the first hash value, is representative of the **licensors** 's digital signature. The
private key , for example RSA-KEYX **manufactured** by RSA, Inc., preferably utilizes an asymmetric **algorithm** . The **license** signature derived at block 2 1 0 is then added to the first hash value...
? t16/5,k/13-14,17-20

16/5,K/13 (Item 13 from file: 349)

00923011 **Image available**

SECURE EXTENSIBLE COMPUTING ENVIRONMENT
ENVIRONNEMENT INFORMATIQUE EVOLUTIF SECURISE

Patent Applicant/Assignee:
TETRAWAVE INC, 955 Massachusetts Avenue, Suite 169, Cambridge, MA 02110-2804, US, US (Residence), US (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
THOMA Johannes, An der Scheibenwiese 1/1/2, A-1160 Vienna, AT, AT (Residence), AT (Nationality), (Designated only for: US)
MURPHY Shawn, 46 Prospect Street, Marblehead, MA 01945, US, US (Residence), US (Nationality), (Designated only for: US)
SCHALLHARDT Christian, Rosensteingasse 44/5, A-1170 Vienna, AT, AT (Residence), AT (Nationality), (Designated only for: US)
Legal Representative:
MAHONEY Denis G (agent), Fish & Richardson, P.C., 225 Franklin Street, Boston, MA 02110-2804, US,

Patent and Priority Information (Country, Number, Date):
Patent: WO 200256528 A2-A3 20020718 (WO 0256528)
Application: WO 2002US422 20020109 (PCT/WO US0200422)
Priority Application: US 2001260543 20010109; US 2001262157 20010117; US 200241772 20020108
Parent Application/Grant:
Related by Continuation to: US 2001260543 20010109 (CON); US 2001262157 20010117 (CON); US 200241772 20020108 (CON)
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG US UZ VN YU ZA ZM ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04L-009/00
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 9203

English Abstract
A method of downloading encrypted e-content to a terminal device (12) includes receiving a request for encrypted content from a terminal device (12). A content server (18) generates a private symmetric key and encrypts the e-content with the symmetric key . A key server (16) looks up the terminal device (12) public key in a key repository and sends the symmetric key encrypted with the public key of the terminal device (12) to the content server (18). The key server (16) generates a unique license i.d. and produces an entry in a license repository. The content server (16) sends a response to the terminal device (12) including the content encrypted with the symmetric key. Transfer tickets and challenges received from the content server (18) are used to activate the e-content license. Additionally, trading of e-content licenses between users, activation of an e-content license transferred from a giver's terminal device (12) to a borrower's terminal device (12) are also supported. For viewing secure content on a personal computer a secure extensible computing environment is implemented on a personal computer peripheral

card while processing of the content is performed in encrypted form in the computer. The content is delivered in encrypted form to the secure extensible computing environment on the personal computer peripheral card and decrypted therein.

French Abstract

La presente invention concerne un procede de telechargement d'un contenu virtuel vers un dispositif de terminal comportant la reception d'une requete pour un contenu chiffre emanant d'un dispositif de terminal. Le serveur de contenu genere une cle symetrique privee et effectue le chiffrement du contenu virtuel au moyen de la cle symetrique. Un serveur de cle recherche la cle publique du dispositif de terminal dans un referentiel de cles et transmet la cle symetrique chiffree avec la cle publique du dispositif de terminal vers le serveur de contenu. Le serveur de contenu genere un permis unique d'identification et effectue une inscription dans le referentiel de permis. Le serveur de contenu envoie une reponse au dispositif de terminal comprenant le contenu chiffre au moyen de la cle symetrique. Des tickets de transfert et des defis recus a partir du serveur de contenu sont utilises pour activer le permis de contenu virtuel. Par ailleurs, l'echange de permis de contenu entre utilisateurs, l'activation d'un permis de contenu transfere d'un dispositif de terminal d'un donateur a un dispositif de terminal d'un emprunteur peuvent egalement etre effectues. Pour une visualisation de contenu securise sur un ordinateur personnel on met en oeuvre un environnement informatique evolutif securise sur une carte peripherique d'un ordinateur personnel durant le traitement du contenu sous forme chiffree dans l'ordinateur. Le contenu est livre sous forme chiffree dans l'environnement informatique evolutif securise sur la carte peripherique de l'ordinateur personnel et y est decrypte.

Legal Status (Type, Date, Text)

Publication	20020718	A2 Without international search report and to be republished upon receipt of that report.
Examination	20030220	Request for preliminary examination prior to end of 19th month from priority date
Search Rpt	20030424	Late publication of international search report
Republication	20030424	A3 With international search report.
Search Rpt	20030424	Late publication of international search report
Correction	20030918	Corrections of entry in Section 1: under (30) replace "Not furnished" by "10/041,772"; under (63) replace "Not furnished" by "10/041,772"
Republication	20030918	A3 With international search report.

Fulltext Availability:
Detailed Description
Claims

Detailed Description

... device 12 includes producing 132 a new entry in protected table of e-content licenses. **Producing** a new entry causes the ticket 90 counters to be set to zero. The **license key** is decrypted 134 using the device's **private key** , but the **license** is not yet activated. The terminal device 12 produces 136 a new transfer ticket 90a...

Claim

... the terininal device public key in a
key repository;
receiving from the key server the **symmetric key** encrypted with the public **key**
of the terminal device;
generating a unique **license** ID and **producing** a new entry in a license

repository; and
sending a response to the terminal device including the content encrypted with the **symmetric key** .
1 5

2 The method of claim I further comprising:
activating the license to allow...

...21
. The method of claim I wherein the public key is used for encrypting the **symmetric key** .

7 The method of claim I wherein generating a unique license ID further comprises:
generating a unique license ID and **producing** a new entry in the license repository and storing the **license** ID and **symmetric key** in the **license** repository.

8 The method of claim I further comprising:
receiving a request to register the...

16/5,K/14 (Item 14 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00917511 **Image available**
METHOD FOR PROVIDING MULTIMEDIA FILES AND TERMINAL THEREFOR
PROCEDE PERMETTANT DE DISTRIBUER DES FICHIERS MULTIMEDIA ET TERMINAL CORRESPONDANT
Patent Applicant/Assignee:
NOKIA CORPORATION, Keilalahdentie 4, FIN-02150 Espoo, FI, FI (Residence), FI (Nationality)
NOKIA INC, 6000 Connection Drive, Irving, TX 75039, US, US (Residence), US (Nationality), (Designated only for: LC)
Inventor(s):
NII Naoaki, 3-12-4-105 Sengen-cho, Higashikurume-shi, Tokyo 203-0012, JP,

Legal Representative:
STOUT Donald E (et al) (agent), Antonelli, Terry, Stout & Kraus, LLP, Suite 1800, 1300 N. Seventeenth Street, Arlington, VA 22209, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200250642 A2-A3 20020627 (WO 0250642)
Application: WO 2001IB2113 20011108 (PCT/WO IB0102113)
Priority Application: US 2000739797 20001220
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PH PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: G06F-001/00
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 13783

English Abstract
A method of and a system for securely distributing data files to a user. A first key is encrypted using a second key. The encrypted first key is stored on an integrated circuit card that is associated with the user. The integrated circuit card is provided to the user. Data files are encrypted using the first key to get an encrypted data file at a first party. The encryption parameters are exchanged between the first party and integrated circuit card.

French Abstract
L'invention concerne un procede et un systeme permettant de distribuer des fichiers de donnees de facon securisee a un utilisateur. Une premiere cle est chiffree a l'aide d'une seconde cle. La cle chiffree est stockee sur une carte a circuit integre associee a l'utilisateur. Cette carte a circuit integre est fournie a l'utilisateur. Les fichiers de donnees sont chiffres a l'aide de la premiere cle afin d'obtenir un fichier de donnees chiffre au niveau d'un premier usager. Les parametres de chiffrement sont echanges entre le premier usager et une carte a circuit integre.

Legal Status (Type, Date, Text)
Publication 20020627 A2 Without international search report and to be republished upon receipt of that report.
Search Rpt 20031113 Late publication of international search report
Republication 20031113 A3 With international search report.
Republication 20031113 A3 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

Fulltext Availability:
Detailed Description

Detailed Description
... administrator generates a pair of the public key (Ki-S 1 -Pu) 105 and the **private key** (Ki-S I Pr) 107. Publisher 100, which may have a **license** agreement with the administrator, receives the public **key** (Ki-S 1 -Pu) 105 in a secure manner. The **manufacturer** of secure module 123, who may have a **license** agreement with the administrator, receives the **private key** (Ki-S 1 -Pr) 107, Publisher 1 00 and the **manufacturer** of secure module 123 may only know one of the pair respectively. Under a license...

...have algorithms A-S 1 103 and A-S2 102, and one 1 0 public **key** 105. Under **license** , the publisher 100 may generate an encrypted **key** (Ki-P2) 108 with algorithm (A-S 1) 103. The **manufacturer** of secure module 123 incorporates two algorithms (A-S 1) 103 and (A-S2) 102, and **private key** (Ki-S1 -Pr) 107 into secure module 123. Publisher 100 encrypts data file IO 1...

16/5,K/17 (Item 17 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00841904 **Image available**
DIGITAL RIGHTS MANAGEMENT WITHIN AN EMBEDDED STORAGE DEVICE
GESTION NUMERIQUE DE DROITS DANS UN DISPOSITIF DE MEMOIRE INTEGRE
Patent Applicant/Assignee:
DATAPLAY INC, 2560 55th Street, Boulder, CO 80301-5706, US, US (Residence), US (Nationality)

Inventor(s):
LEE Lane W, 894 S. Bermont Drive, Lafayette, CO 80026, US,
ZAHARRIS Daniel R, 7329 Mt. Meeker Road, Longmont, CO 80503, US,
Legal Representative:
STEUBER David E (et al) (agent), Skjerven Morrill MacPherson LLP, 25 Metro Drive, Suite 700, San Jose, CA 95110, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200175562 A2-A3 20011011 (WO 0175562)
Application: WO 2001US10405 20010329 (PCT/WO US0110405)
Priority Application: US 2000542510 20000403
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: G06F-001/00
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 9881

English Abstract
A method is provided for enabling locked data stored on a storage medium and accessing it through a data storage engine contained within or connected to a host device. A user selects all or part of the data stored on the storage medium to enable. The host device then connects to a server over a network and completes a transaction. The transaction can be any requirement specified by the supplier of the data selected by the user. Once the transaction is complete, the data storage engine connects to the same or a separate server through the host device and receives a piece of information, known as the content key, necessary to decrypt, read, or otherwise make sense of the data selected by the user. The content key may be, for example, part of a decryption key. The content key is combined with other information stored on the storage medium. The combined information is then used to access the data selected by the user.

French Abstract
L'invention concerne un procede permettant d'activer des donnees verrouillees enregistrees sur un support de memoire et d'y acceder par un moteur de stockage des donnees integre ou relie a un dispositif hote. L'utilisateur selectionne tout ou partie des donnees enregistrees sur le support de memoire aux fins d'activation. Ensuite, le dispositif hote se connecte a un serveur sur un reseau et etablit une transaction pouvant correspondre a telle ou telle exigence specifiee par le fournisseur des donnees selectionnees par l'utilisateur. Une fois la transaction etablie, le moteur de stockage des donnees se connecte au meme serveur ou a un autre serveur via le dispositif hote et recoit un element d'information, appele cle de contenu, necessaire pour toute operation de dechiffrement, lecture ou autre comprehension des donnees selectionnees par l'utilisateur. Par exemple, cette cle peut faire partie integrante d'une cle de dechiffrement. Ladite cle est combinee a d'autres informations stockees sur le support de memoire. L'information ainsi combinee est ensuite utilisee pour l'acces aux donnees selectionnees par l'utilisateur.

Legal Status (Type, Date, Text)
Publication 20011011 A2 Without international search report and to be republished upon receipt of that report.
Examination 20020110 Request for preliminary examination prior to end of 19th month from priority date
Search Rpt 20020906 Late publication of international search report
Republication 20020906 A3 With international search report.

Fulltext Availability:
Detailed Description

Detailed Description
... to form a new packet. hi stage 410, the new packet is encrypted using a **secret symmetric key** . The **secret symmetric keys** are generated by the entity that **manufactures** the data storage engine and **licenses** the content **key** server to sell storage media that can be read by the data storage engine. In one embodiment, the **secret symmetric keys** are three triple-DES keys and the new packet is encrypted using triple-DES. The...
...encrypted using a public engine key. The public engine key is part of a public/ **private key** pair generated by the entity that **manufactures** the data storage engine 14. The public engine key is given to the content **key** server when the content **key** server is **licensed** by the **manufacturing** entity.

1 5 In stage 428, the data packet forined in stage 424 is encrypted...

...concatenated to form another data packet. The server certificate is also issued to the content **key** server by the **manufacturing** entity during server **licensing** , and is signed by a private **key** which is part of a public/ **private key** pair held by the **manufacturer** . In stage 432, the packet formed in stage 430 is signed with a digital signature using the **private** server **key** . The **private** server **key** is part of a public/ **private key** pair and is given to the content **key** server during **licensing** by the **manufacturing** entity. In stage 434, the data packet formed in stage 430 is concatenated with the...provides the Engine with the
Server's Public Key (P.)
Manufacturer. 163 This is a **private key** that will only be held by the **Private Key** manufacturer, and will be used to create Server Certificates
for licensed Servers.

Manufacturer 168 This is a symmetric TDES-CBC key that will be issued to
TDES-CBC **Key** all **licensed** Engines and Servers.

Engine Public 326 This is a public key that will be issued...

...TDES-CBC Key TDES-CBC key for communicating with the server.

Server Public 326 Each **licensed** Server will be issued a public **key** by the **Key manufacturer** .

Server Private 163 Each **licensed** Server will be issued a **private key**0 by the **Key manufacturer** .

Server 326+ Each **licensed** Server will be issued a Server Certificate that
Certificate 160 will be used by the...

16/5,K/18 (Item 18 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00818548 **Image available**

DIGITAL RIGHTS MANAGEMENT SYSTEM OPERATING ON COMPUTING DEVICE AND HAVING BLACK BOX TIED TO COMPUTING DEVICE

SYSTEME DE GESTION DES DROITS NUMERIQUES S'EXECUTANT SUR UN DISPOSITIF INFORMATIQUE, LA BOITE NOIRE DUDIT SYSTEME ETANT LIEE AU DISPOSITIF INFORMATIQUE

Patent Applicant/Assignee:
MICROSOFT CORPORATION, One Microsoft Way, Redmond, WA 98052, US, US (Residence), US (Nationality)
Inventor(s):
PEINADO Marcus, 5007 148th NE, E207, Bellevue, WA 98007, US,
LIU Donna, 15720 SE 44th Place, Bellevue, WA 98006, US,
GANESAN Krishnamurthy, 17345 NE 65th Way, Redmond, WA 98052, US,
Legal Representative:
ROCCI Steven J (et al) (agent), Woodcock Washburn Kurtz Mackiewicz & Norris LLP, 46th floor, One Liberty Place, Philadelphia, PA 19103, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200152021 A1 20010719 (WO 0152021)
Application: WO 2000US23108 20000822 (PCT/WO US0023108)
Priority Application: US 2000176425 20000114; US 2000526290 20000315
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: G06F-001/00
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 36187

English Abstract
A digital rights management (DRM) system operates on a computing device (14) when a user requests that an encrypted piece of digital content be rendered by the computer device (14). The computing device (14) has an identifier. A black box (30) performs decryption and encryption functions in the DRM system. The black box (30) includes a key file and an executable. The key file includes at least one black box public key and is expected to include the identifier of the computing device (14), the black box (30) thus being tied to the computing device (14) by inclusion of such first identifier. A digital license (16) corresponding to the digital content is resident in the DRM system and includes a decryption key for decrypting the encrypted digital content. The decryption key is expected to be encrypted according to the black box public key of the key file of the black box (30), the license (16) thus being tied to the black box (30) and by extension the computing device (14). If the identifier of the computing device (14) is in fact different than the identifier in the key file of the black box (30), a different key file is produced based on the black box public key(s) of the key file and the different identifier of the computing device (14).

French Abstract
L'invention concerne un systeme de gestion des droits numeriques (DRM) s'executant sur un dispositif informatique (14) lorsqu'un utilisateur demande qu'une partie cryptee d'un contenu numerique soit remise par ledit dispositif informatique (14). Le dispositif informatique (14) possede un identificateur. Une boite noire (30) assure les fonction de decryptage et de cryptage dans le systeme DRM. Ladite boite noire (30) comprend un fichier de cles et un fichier executable. Le fichier de cles renferme au moins une cle publique de boite noire et il est cense renfermer l'identificateur du dispositif informatique (14), ladite boite noire (30) etant ainsi liee au dispositif informatique (14) du fait de l'inclusion de ce premier identificateur. Une licence numerique (16) correspondant au contenu numerique et residant dans le systeme DRM comprend une cle de decryptage destinee au decryptage du contenu numerique crypte. La cle de decryptage est normalement cryptee selon une cle publique de boite noire du fichier de cles de la boite noire (30), la licence (16) etant ainsi liee a la boite noire (30), et par extension, au dispositif informatique (14). Si l'identificateur du dispositif informatique (14) s'avere different de l'identificateur contenu dans le fichier de cles de la boite noire (30), un fichier de cles different est produit en fonction des cles publiques de boite noire du fichier de cles et de l'identificateur different du dispositif informatique (14).

Legal Status (Type, Date, Text)
Publication 20010719 A1 With international search report.
Examination 20011004 Request for preliminary examination prior to end of 19th month from priority date

Fulltext Availability:
Claims
Claim
... encrypted
according to the different black box public key;
applying the extracted different black box **private key** to the extracteddecryptionkeyencryptedaccordingtothedifferentblackboxpublickeyto produce the decryption key;
encrypting the produced decryption key according to the received current black box public **key** ;
producing the different **license** having the encrypted decryption **key** ; and
forwarding the different **license** to the computing device and the DRM system thereof for appropriate installation thereon.

31 The method of claim 29 comprising perfonning the receiving, **producing** , and forwarding steps by a license re-writing device external to the computing device.

32...

16/5,K/19 (Item 19 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00763274
DIGITAL PRODUCT LICENSE CONTROL SYSTEM BASED ON INDEPENDENT DIGITAL PRODUCT REGISTRATION SERVER
SYSTEME DE CONTROLE DE PERMIS D'UTILISATION DE PRODUIT NUMERIQUE UTILISANT **UN SERVEUR INDEPENDANT D'ENREGISTREMENT DE PRODUIT NUMERIQUE**

Patent Applicant/Inventor:
PARK Hyo Joon, Kwacheon Jugong Apt. 408-504, 7, Byalyang-dong,
Kwacheon-si, Kyungki-do 427-040, KR, KR (Residence), KR (Nationality)
Patent and Priority Information (Country, Number, Date):
Patent: WO 200075787 A1 20001214 (WO 0075787)
Application: WO 99KR277 19990605 (PCT/WO KR9900277)
Designated States: JP KR US
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Main International Patent Class: G06F-012/14
International Patent Class: H04L-009/00
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 3582

English Abstract
The registration server is independent of digital product manufacturers and open to all digital product manufacturers. The manufacturer registers his digital product to the server and gets product registration file of the product from the server. The product manufacturer merges the product and the product registration file and encrypts them using manufacturer digital product license control program. If a public digital product is executed on user computer, said digital product is linked to digital product execution program which is subsystem of user digital product license control program. The program decrypts said digital product and reads the product ID from the product registration file and checks the license file received from a digital product registration server. If there is no license for the digital product, said program asks the user to buy a license of the product.

French Abstract
Ce serveur d'enregistrement, qui est independant des fabricants de produits numeriques, est accessible a tous les fabricants de produits numeriques. Le fabricant enregistre son produit numerique aupres du serveur et en recoit un fichier d'enregistrement de produit. Le fabricant joint le produit au ficher d'enregistrement et les chiffre a l'aide d'un programme de controle de permis d'utilisation de produit numerique. Si un produit numerique a usage public est execute sur un ordinateur d'utilisateur, il est lie au programme d'execution de produit numerique qui est un sous-systeme du programme de controle de permis d'utilisation de produit numerique. Le programme dechiffre ledit produit numerique, lit l'identificateur du produit dans le fichier d'enregistrement de produit et verifie le fichier de permis d'utilisation emanant du serveur d'enregistrement de produit numerique. Si aucun permis d'utilisation du produit numerique n'a ete etabli, ce programme invite l'utilisateur a l'acquerir.

Legal Status (Type, Date, Text)
Publication 20001214 A1 With international search report.
Examination 20010308 Request for preliminary examination prior to end of 19th month from priority date

Fulltext Availability:
Claims

Claim
... key to said registration server and receiving the
public key of said registration server.
registering **manufacturer** once per **manufacture** to the cen tral digital

product registration server and receiving partial user-ID file from dicrital product registration server. **Manufacturer** digital product **license** control program attaches the **manufacturer** **secret** /public **key** pair and the public key of central dicrital product registration server to the partial user-ID file that
tD
includes **manufacturer** information encrypted by **manufacturer** public key
and digital signed by the sever **secret** **key** .
registering digital product, with player information, to central digital product registration server and receiving product...

16/5,K/20 (Item 20 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00484595
SOFTWARE LICENSE CONTROL SYSTEM BASED ON INDEPENDENT SOFTWARE REGISTRATION SERVER
SYSTEME DE VERIFICATION DE PERMIS D'UTILISATION DE LOGICIEL UTILISANT UN SERVEUR INDEPENDANT D'ENREGISTREMENT DE LOGICIELS
Patent Applicant/Assignee:
PARK Hyo Joon,
Inventor(s):
PARK Hyo Joon,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9915947 A1 19990401
Application: WO 97KR175 19970919 (PCT/WO KR9700175)
Priority Application: WO 97KR175 19970919
Designated States: JP US AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Main International Patent Class: G06F-001/00
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 2348
English Abstract
The registration servers are independent of software product manufacturers and open to all software manufacturers. On user computer, software product asks user software license control program whether the user has usage license for the software product. The user license control program checks the license file, which was received from a software registration server, and answers the software product. If the answer is "no", the software product stops running. If the answer is "yes", it continues. Said license file cannot be used by unauthorized user because said file is encrypted by the user public key and digital signed by the secret key of a software registration server. To use a license file, user needs the secret key of the user and needs passphrase to activate the secret key. The license file is digital signed by software registration server and cannot be modified by a user to add unauthorized license. There are 3 types of registration need to be done by user. User registration, CPU registration and software product usage license registration. User does user registration for himself once per person. After that, the user registers his CPU once per CPU. User registers software product usage license once per every product of specific CPU. On user registration, the user gets partial user-ID file from the software registration server. After receiving the partial user-ID file, user software license control program attaches public/secret key pair of the user and public key of the registration server of the user to the partial

user-ID file. This user-ID file is essential in registering CPU and purchasing software product. The user-ID file is independent of any CPU and this file need to be copied to all of his CPUs. On CPU registration, user gets license file from software registration server. And the license file is updated every time the user purchases new software product or upgrades a software product. The software product information is added to the license file every time new product is purchased or a product is upgraded. Also because of expiration date, the license file is refreshed periodically. Software product usage license is given to a specific CPU of a specific user. The license file is dependent on a specific CPU. The license file is given to a specific CPU of a specific user. Both the user-ID file and license file is encrypted by user public key and digital signed by software registration server secret key. So, only the registration server can modify said files.

French Abstract

Les serveurs d'enregistrement sont independants des fabricants de produits logiciels et ouverts a tous les fabricants de logiciels. Sur l'ordinateur de l'utilisateur, le produit logiciel demande au programme de verification de permis d'utilisation de logiciel si l'utilisateur possede le permis d'utilisation associe au produit logiciel. Le programme de verification de permis de l'utilisateur verifie le fichier des permis d'utilisation, qui a ete recu d'un serveur d'enregistrement de logiciels, et repond au produit logiciel. Si la reponse est "non", le produit logiciel cesse de s'executer. Si la reponse est "oui", il continue. Ledit fichier de permis ne peut pas etre utilise par un utilisateur non autorise car ce fichier est chiffre avec la cle publique de l'utilisateur et signe numeriquement avec la cle secrete d'un serveur d'enregistrement de logiciels. Pour utiliser un fichier de permis, l'utilisateur a besoin de connaitre la cle secrete et a besoin d'une phrase passe pour activer cette cle secrete. Le fichier de permis est signe numeriquement par le serveur d'enregistrement de logiciels et ne peut pas etre modifie par un utilisateur qui souhaiterait ajouter un permis non autorise.
L'utilisateur peut avoir recours a trois sortes d'enregistrement: un enregistrement utilisateur, un enregistrement d'unite centrale et un enregistrement de permis d'utilisation de produit logiciel. Chaque utilisateur effectue une seule fois un enregistrement utilisateur. Apres cela, l'utilisateur enregistre une seule fois son unite centrale. L'utilisateur enregistre un permis d'utilisation de logiciel, une fois pour chaque logiciel, sur une unite centrale particuliere. Lors de l'enregistrement utilisateur, l'utilisateur recoit un fichier d'identification utilisateur partiel qui lui est transmis par le serveur d'enregistrement des logiciels. Apres reception du fichier d'identification utilisateur partiel, le programme de verification de permis d'utilisation de logiciel attache la paire de cles publique/secrete de l'utilisateur et la cle publique du serveur d'enregistrement de l'utilisateur au fichier d'identification utilisateur partiel. Ce fichier d'identification utilisateur partiel est essentiel a l'enregistrement de l'unite centrale et a l'achat du produit logiciel. Ce fichier d'identification utilisateur partiel est independant de toute unite centrale et il doit etre copie sur chacune des unites centrales. Lors de l'enregistrement de l'unite centrale, l'utilisateur obtient le fichier de permis du serveur d'enregistrement des permis. Et le fichier de permis est mis a jour chaque fois que l'utilisateur achete un nouveau produit logiciel ou fait evoluer un produit logiciel. Des informations relatives au produit logiciel sont ajoutees au fichier de permis chaque fois qu'un nouveau produit logiciel est achete ou qu'un produit evolue. Aussi, en raison de la date d'expiration, le fichier de permis est rafraichi periodiquement. Ce fichier de permis est dependant d'une unite centrale particuliere. Il est donne a une unite centrale particuliere d'un utilisateur particulier. Le fichier d'identification utilisateur et

le fichier de permis sont tous deux chiffres avec la cle publique de l'utilisateur et signe numeriquement avec la cle secrete du serveur d'enregistrement des logiciels. De cette maniere, seul le serveur d'enregistrement a la possibilite de modifier ces fichiers.

Fulltext Availability:
Detailed Description

Detailed Description
... because said file is encrypted by the user public key and digital signed by the **secret key** of a software registration server. To use a license file, user needs the **secret key** of the user and needs passphrase to activate the **secret key** . The **license** file is digital signed by software
registration server and cannot be modified by a user to add unauthorized license.

All software product **manufacturers** register their products to the central software registration server. The central registration server distributes the...server is open to all software product manufacturers and is not just for one software **manufacturer** .

. registering user once per person to the software registration server and receiving partial software registration server. User software **license** control program attaches the user **secret** /public **key** pair and the public key of the user's software registration server to the partial
...
?